

WHAT IS CLAIMED IS:

Sub are

1. A parallel counter comprising:
 a plurality of inputs for receiving a binary number as a plurality of binary inputs;
 a plurality of outputs for outputting binary code indicating the number of binary ones in the plurality of binary inputs; and
 a logic circuit connected between the plurality of inputs and the plurality of binary outputs and for generating each of the plurality of binary outputs as a symmetric function of the binary inputs. *? (1)*

Fig. 11

2. A parallel counter according to claim 1 wherein said logic circuit is arranged to generate at least one of the binary outputs as a symmetric function of the binary inputs using exclusive OR logic for combining a plurality of sets of one or more binary inputs.

Fig. 9
but not part of parallel counter

3. A parallel counter according to claim 2 wherein said logic circuit is arranged to logically AND members of each set of binary inputs and to logically exclusively OR the result of the AND operations. *(12) min - design Where is Dwyg?*

4. A parallel counter according to claim 3 wherein said logic circuit is arranged to logically AND 2^i of the binary inputs in each set for the generation of the i^{th} binary output, where i is an integer from 1 to N , N is the number of binary outputs and i represents the significance of each binary output, each set being unique and the sets covering all possible combinations of binary inputs. *(12) 2-5 x 2-9*

5. A parallel counter according to claim 3 wherein said logic circuit is arranged to logically AND members of each set of binary inputs, where each set is unique and the sets cover all possible combinations of binary inputs.

6. A parallel counter according to claim 1 wherein said logic circuit is arranged to generate at least one of the binary outputs as a symmetric function of the binary inputs using OR logic for combining a plurality of sets of one or more binary inputs.

~~7. A parallel counter according to claim 6 wherein said logic circuit is arranged to logically AND members of each set of binary inputs and to logically OR the result of the AND operations.~~

Sub 2
~~8. A parallel counter according to claim 7 wherein said logic circuit is arranged to logically AND 2^{N-1} of the binary inputs in each set for the generation of the N^{th} binary output, where N is the number of binary outputs and the N^{th} binary output is the most significant, each set being unique and the sets covering all possible combinations of binary inputs.~~

~~9. A parallel counter according to claim 7 wherein said logic circuit is arranged to logically AND members of each set of binary inputs, where each set is unique and the sets cover all possible combinations of binary inputs.~~

Sub 1
~~10. A parallel counter according to claim 1 wherein said logic circuit is arranged to generate a first binary output as a symmetric function of the binary inputs using exclusive OR logic for combining a plurality of sets of one or more binary inputs, and to generate an N^{th} binary output as a symmetric function of the binary inputs using OR logic for combining a plurality of sets of one or more binary inputs.~~

~~11. A parallel counter according to claim 1 wherein said logic circuit is arranged to generate two possible binary outputs for a binary output less significant than the N^{th} binary output, as symmetric functions of the binary inputs using OR logic for combining a plurality of sets of one or more binary inputs where N is the number of binary outputs, the sets used for each possible binary output being of two different sizes which are a function of the binary output being generated; and said logic circuit including selector logic to select one of the possible binary outputs based on a more significant binary output value.~~

(12)
min-class-
cryption
e.g. A, B,
not generated
crypto portion
in 15

Subj and
308
enough
for CPA

(4)
 mis-
 desnylin
 note Fri 17
 logic is

5-8-18

9 min - down
when in
the danger

~~SECRET~~

KND C